明 細 書

プログラマブルロジックコントローラの周辺装置

技術分野

[0001] この発明は、プログラマブルロジックコントローラ(以下、PCと称す)と通信可能なPCのプログラミングを行う周辺装置に関するものである。

背景技術

[0002] 従来のPCの周辺装置は、PCと直接接続ケーブルを経由して接続され、利用される。このときPCに登録されているデータの読み出し・書き込みを制限するために、PCは認証手段を備えている。認証手段では、任意の文字で構成される認証データをPC内のデータに設定することができる。データが複数存在する場合は個々のデータに対して別々の認証データを設定することが可能である。

[0003] PCの周辺装置からPC内の認証データが設定されたデータを読み出し・書き込みするためには、周辺装置の入力手段にてPCに設定された認証データと同一の認証データを入力する必要がある。入力が一致しない場合は認証が許可されず、データに対して読み書きを実施することはできない。

[0004] また、PCと周辺装置はネットワークを経由して接続することができる。このとき，PCへのネットワーク経由アクセスを制限するために、PCの認証手段を利用することができる。認証機能には、ネットワーク経由で接続するための認証データが設定される。ネットワーク経由でPCと接続する周辺装置の利用者は、そのデータに対して読み書きができるようにするために入力装置にて登録された認証データと同一の認証データを入力する必要がある。

[0005] PC内の認証データの設定自体は、PCに接続ケーブル経由で周辺装置の入力手段から任意の認証データを入力し、PCに登録することで実施する。このとき、既に認証データが設定されていたら、周辺装置の入力装置にてPCに設定された認証データと同一の認証データを入力してPCの認証許可を得た後、新しい認証データ12を設定することができる。

[0006] 従来の技術の例として日本国特許出願公開番号 特開平10−124308号に記載

の技術がある。

特開平10—124308号に記載の技術によれば、例えばPCの運転に必要なプログラムや設定値といった情報は、システムの所有者にとってシステム運用のためのノウハウが蓄積された情報資産である。そして、情報資産が含まれているデータに対し、第三者への漏洩には細心の注意を払う必要があることから、情報資産の漏洩を守るという観点で、プログラム中に保護用の命令を埋め込むことで、PCの命令語を暗号化し解除キーを持たない利用者には命令を不可視にするといった方法がある。

[0007] 特許文献1:日本国特許出願公開番号 特開平10—124308号

発明の開示

発明が解決しようとする課題

[0008] 特開平10—124308号に記載の技術であっても認証データを知る利用者の誤操作あるいは明確な悪意によるデータ漏洩のリスクを否定できないといった問題があり、その対策として、例えば定期的に認証データを更新することや、認証データを複雑にするといったものがあげられる。しかし、一般にこのような対策は周辺装置の利用者の負荷増大を招き、装置利用時の利便性と相反するといった問題もあった。

[0009] この発明は、認証データの漏洩に伴う不正操作及び情報資産であるデータの漏洩を防止するために、装置利用時の利便性を損なわず、周辺装置の利用者に認証データおよびデータの中身を公開する必要のないPCの周辺装置を提供することを目的とする。

課題を解決するための手段

[0010] この発明は、プログラマブルロジックコントローラの周辺装置自体の使用許可の認証に使用される周辺装置認証データ、プログラマブルロジックコントローラ内で使用されるデータ、及び前記プログラマブルロジックコントローラにて設定され、前記データに対してプログラマブルロジックコントローラとの通信可否を認証する認証データを暗号化する暗号化手段と、少なくとも暗号化された前記周辺装置認証データを記憶する外部記憶手段と、少なくとも暗号化された前記周辺装置認証データを記憶する内部記憶手段と、前記周辺装置認証データ、前記データ、前記認証データを復号化する復号化手段と、前記外部記憶手段、前記内部記憶手段から読み出され、復号化さ

れた各々の前記周辺装置認証データを照合してプログラマブルロジックコントローラの周辺装置の使用可否を判別する照合手段とを備えたものである。

発明の効果

[0011] この発明は、プログラマブルロジックコントローラの周辺装置自体の使用許可の認証に使用される周辺装置認証データ、プログラマブルロジックコントローラ内で使用されるデータ、及び前記データに対してプログラマブルコントローラとの通信可否を認証する認証データを暗号化する暗号化手段と、少なくとも暗号化された前記周辺装置認証データを記憶する外部記憶手段と、少なくとも暗号化された前記周辺装置認証データを記憶する内部記憶手段と、前記周辺装置認証データ、前記前記データ、前記認証データを復号化する復号化手段と、前記外部記憶手段、前記内部記憶手段から読み出された各々の復号化された前記周辺装置認証データを照合してプログラマブルロジックコントローラの使用可否を判別する照合手段とを備えたので、装置利用時の利便性を損なわず、周辺装置の利用者に認証データおよびデータの中身を公開する必要のないプログラマブルロジックコントローラの周辺装置を提供することができる。

図面の簡単な説明

[0012] [図1]本発明の実施例1のPC1とPC1の周辺装置の構成を示す構成図である。

[図2]本発明の実施例1におけるのPC1を利用可能とする周辺装置認証データ16の設定時の説明図である。

[図3]図2の説明図のフローチャートである。

[図4]本発明の実施例1におけるのPC1を利用可能とする周辺装置認証データ16の照合手段13での照合の説明図である。

[図5]図4の説明図のフローチャートである。

[図6]本発明の実施例1におけるのPC1利用可能後のデータ4の生成の説明図である。

[図7]図6の説明図のデータ4の書き込み時フローチャートである。

[図8]図6の説明図のデータ4の読み込み時のフローチャートである。

[図9]本発明の実施例1におけるのPC1へのデータ4の新規登録時の説明図である。

[図10]図9の説明図のフローチャートである。

[図11]本発明の実施例1におけるのPC1へのデータ4の読み出し、照合、更新時の説明図である。

[図12]図11の説明図のフローチャートである。

[図13]本発明の実施例1におけるのPC1へのデータ4の読み出し、照合、更新時の説明図である。

[図14]図13の説明図のフローチャートである。

[図15]本発明の実施例1におけるのPC1へのデータ4の読み出し、照合、更新時の説明図である。

[図16]図15の説明図のフローチャートである。

符号の説明

[0013] 1 PC、2 記憶手段、3 認証データ、4 データ、5 認証手段、6 接続ケーブル、7 ネットワーク、8 周辺装置、9 入力手段、10 暗号化手段、11 内部記憶手段、12 復号化手段、13 照合手段 14 外部記憶通信手段、15 外部記憶手段、16 周辺装置認証データ、17 暗号化周辺装置認証データ、18 ネットワーク認証データ。

発明を実施するための最良の形態

[0014] 発明を実施するための最良の形態を、実施例1及び実施例2にて説明する。

実施例 1

[0015] 図1は、本発明の実施例1のPC1とPC1の周辺装置の構成を示す構成図である。

PC1は、PC1内の記憶手段2は、認証データ3及びデータ4を記憶する機能を有している。また、PC1は、認証手段5を備えており、認証手段5は、記憶手段2と情報伝達可能であると共に、通信手段であるPC1の通信手段である接続ケーブル6または電気通信回線等のネットワーク7にも情報伝達可能に配設されている。認証手段5は、接続ケーブル6または電気通信回線等のネットワーク7を介して、PC1内に登録されているデータ4の読み出し・書き込みを行おうとする行為に対し、データ4の読み出し・書き込みの許可を与えるものであり、認証データ3と同じデータが入力されたか否かによってその許可の判断を行う。データ4は、PCの運転に必要なプログラムや設定

値といった情報であり、これはPCからなるシステムの所有者にとってはシステム運用のためのノウハウが蓄積された情報資産である。

[0016] また、認証手段5では、認証データ3を任意の文字で構成させることができ、また、データ4が複数存在する場合は個々のデータに対して別々の認証データ3を設定することが可能である。

[0017] 周辺装置8は、任意の認証データ3やデータ4を作成する入力手段9と、入力手段9によって入力された認証データ3やデータ4を暗号化する暗号化手段10と、暗号化手段によって暗号化された認証データ3やデータ4を記憶する内部記憶手段11とを備えている。

また、暗号化手段10は、外部記憶通信手段14を介して周辺装置8の外部に存在する外部記憶手段15と情報伝達が可能であり、暗号化された認証データ3やデータ4を記憶させることができる。

[0018] 内部記憶手段11または外部記憶通信手段14を介して周辺装置8の外部に存在する外部記憶手段15に記憶された暗号化された認証データ3やデータ4を復号する復号化手段12と、復号化手段12にて復号化された内部記憶手段11の認証データ3と外部記憶手段15の認証データ3とを照合して、認証されれば認証手段5に対し、データ3の読み出し・書き込みを可能にする照合手段13とから構成されている。

[0019] 動作について説明する。

周辺装置8からPC1内の認証データ3が設定されたデータ4を読み出し・書き込みするためには、周辺装置8の入力手段9にてPC1に設定された認証データ3と同一の認証データを入力する必要がある。入力が一致しない場合は認証が許可されず、データに対して読み書きを実施することはできない。

[0020] そこで、まずPC1および周辺装置8を最初に利用する際に、PC1へのアクセス制御ための認証情報の設定を行う。図2は、本発明の実施例1におけるのPC1を利用可能とする周辺装置認証データ16の設定時の説明図である。また、図3に図2の説明図のフローチャートを示す。尚、以下実施例1についての説明においては、ネットワーク環境下を無視して説明する。

PC1および周辺装置8の利用者は、まず周辺装置8の外部記憶通信手段14と、外

部記憶手段15との情報通信を可能にする。図3においては、周辺装置8を起動し(S101)、認証情報の設定の開始(S102)後に、外部記憶通信手段14と外部記憶手段15とを有線、無線問わず電気的に接続し(S103)、外部記憶手段15を利用可能かどうか判別する(S104)。外部記憶手段15が利用可能でない場合は認証情報の設定登録は失敗となる(S110)。

[0021] 外部記憶手段15が利用可能である場合は、入力手段9を用いて新規に登録する周辺装置認証データ16を入力する(S105)。入力された周辺装置認証データ16は暗号化手段10で暗号化され(S106)、暗号化が失敗した場合(S107)は認証情報の設定登録は失敗となる(S110)が、暗号化が成功した場合(S107)は、外部記憶手段15と内部記憶手段11とにそれぞれ暗号化された暗号化周辺装置認証データ17として保存され(S109)、登録成功として終了する(S109)。このとき外部記憶手段14と内部記憶手段17へ記憶される暗号化周辺装置認証データ17はそれぞれ異なる暗号鍵で暗号化される。

[0022] 上記の手順の後、周辺装置8の利用するには、周辺装置認証データ16が必要となる。図4は、本発明の実施例1におけるのPC1を利用可能とする周辺装置認証データ16の照合手段13での照合の説明図である。また、図5は、図4の説明図のフローチャートである。

図4、5において、周辺装置8の利用者は、周辺装置8の利用開始後(S111)、暗号化周辺装置認証データ17が登録された外部記憶手段15を周辺装置8の外部記憶通信手段14と通信可能(S112)とする。周辺装置8は、外部記憶手段15に暗号化周辺装置認証データ17が存在することを確認し(S113)、および内部記憶手段12に暗号化周辺装置認証データ17があることを確認し(S114)、両者を復号化手段12で復号化した後(S115)、照合手段13にて復号化した結果を照合する(S116)。照合結果が一致したときのみ周辺装置8の利用が許可(S117)される。外部記憶手段15または内部記憶手段10が利用不可または暗号化周辺装置認証データ17がない場合(S113、S114)や、それらの復号に失敗した場合および照合結果が一致しない場合(S116)のいずれかであったなら周辺装置8は利用できない(S118)。

[0023] PC1へのアクセスが可能となり、周辺装置8が利用可能となった後のデータ4の生

成ついて説明する。図6は、本発明の実施例1におけるのPC1利用可能後のデータ4の生成の説明図である。また、図7は、図6の説明図のデータ4の書き込み時フローチャートであり、図8は、図6の説明図のデータ4の読み込み時のフローチャートである。

[0024] 図6、7において、利用者が周辺装置8の入力手段9を用いて作成し、入力完了(S122)したデータ4は、暗号化した後(S123)、暗号化が成功したか否かを確認してから(S124)、内部記憶手段11または外部記憶手段15に保存され(S125)、その保存が成功したか否かを確認し(S126)、成功していればデータ4の保存は成功となる(S127)。S124の暗号化またはS126のデータ4の保存が失敗してれば、データ保存は失敗(S128)となる。尚、図6では、外部記憶手段15にて記憶された場合のみを示している。

[0025] また、図6、8において、利用者が周辺装置8の内部入力手段12または外部記憶手段15から暗号化されているデータ4を復号化手段12に読み込み(S132)、暗号化されたデータ4が成功したか否かを確認してから(S133)、復号化手段12によって復号化され、(S134)、その復号化が成功したか否かを確認し(S135)、成功していればデータ4の読み込みは成功となる(S136)。S133の読み込みまたはS135のデータ4の復号化が失敗してれば、読み込みは失敗(S137)となる。

[0026] よって、内部記憶手段11または外部記憶手段15に保存された暗号化されたデータ4は、周辺装置8が利用許可状態で有る場合のみ、内部記憶手段11または外部記憶手段15から読み込まれ，復号化手段12で復号化してPC1にデータ4として転送する。

[0027] そして、PC1にデータ4を新規登録する際には新規登録されるデータ4に対し、PC1は、自動的に認証データ3を設定する。図9は、本発明の実施例1におけるのPC1へのデータ4の新規登録時の説明図である。また、図10は、図9の説明図のフローチャートである。外部記憶手段15にある暗号化されたデータ4をPC1に登録する。

[0028] 図9、10において、PC1と周辺装置8の利用者は、周辺装置8の利用が許可されている状態(S141)で、内部記憶手段11または外部記憶手段15に保存された暗号化された認証データ3とデータ4を復号化手段12に読み込んで(S142)、復号化手段1

2にて復号して(S143)、通信手段である接続ケーブル6を介して、PC1に認証データ3とデータ4を送信して登録する。登録が成功したら(S144)、認証手段5にてデータ4に認証データ3を設定し(S145)、その設定が成功したら(S146)データ4の新規登録は成功する(S147)。もし、S144での登録またはS146の設定が成功しなかったらデータ4と認証データ3をPCから消去し(S148)、データ4の新規登録は失敗となる(S149)。

[0029] 尚、周辺装置8を有効にした周辺装置認証データ16とPC1に新規登録するデータ4の認証データ3は別物という前提で説明しているが、PC1がデータ4の認証データ3を設定する際に、認証データ3を個別のデータ4ごとに変更してもよいし、周辺装置認証データ16と同じものに設定してもよい。

[0030] これにより、データ4およびその保護のための認証データ3をPC1にデータを登録する都度、入力手段9にて入力する必要がなくなる。この操作における利用者にデータおよびその認証データを公開することなく、作業を遂行させることができる。また, 従来の周辺装置8をPC1に接続する利用者にとっては従来同様に、外部記憶手段15に正規に記憶された認証データ3を入力しないと、PC1に登録されたデータ4にアクセスできないという効果がある。

[0031] PC1に登録されている認証データ3で保護されたデータ4の読み出し、あるいはデータ4の照合、更新をする際には、認証データ3を自動的に送出する。図11は、本発明の実施例1におけるのPC1へのデータ4の読み出し、照合、更新時の説明図である。図12は、図11の説明図のフローチャートを示す。

[0032] 図11、12において、PC1と周辺装置8の利用者は、周辺装置8の利用が許可されている状態で、PC1内に登録されているデータ4の読み出し、照合、更新を開始することができる(S151)。まず、個々のデータ4が認証データ3で保護されているので、内部記憶手段11または外部記憶手段15から暗号化された認証データ3を読み出し(S152)、復号化手段12で復号化し、PC1に送信する(S153)。PC1の認証手段5は、これがデータ4に関連付けられた認証データ3と一致する場合にPC1内のデータ4を照合、読み出し、あるいは更新することを許可する(S154)。データ4に関連付けられた認証データ3と一致しない場合には、データ4の読み出しは失敗となる(S169

)。

[0033] S154での認証がOKとなった後、データ4を照合する場合(S155)には、データ4をPC1から読み込む(S156)と共に、内部記憶手段11または外部記憶手段15から暗号化されているデータ4を復号化手段12へ読み出し(S157)、復号化手段12にて復号化した後(S158)、照合手段13にて両方のデータ4の比較を行って(S159)のデータの照合が成功すれば作業を終了する(S160)。

[0034] データ4を読み出しする場合(S155)には、データ4をPC1から読み込み(S161)、データ4を暗号化手段10にて暗号化し(S162)、暗号化されたデータ4を内部記憶手段11または外部記憶手段15に保存して(S163)、データの読み出しを成功させる(S164)。

[0035] データ4を更新する場合(S165)には、内部記憶手段11または外部記憶手段15からデータ4を復号化手段に読み出し(S166)、復号化手段12にてデータ4を復号化し、(S167)、復号化されたデータ4を通信手段である接続ケーブル6を介してPC1に登録することで更新される(S168)。その際、更新するデータ4に関連する認証データ3は、前回と同一でもよいし、更新時に新たな認証データ3に変更してもよい。

[0036] これにより、認証データ3で保護されたデータ4の読み出し・照合・更新の都度、認証データ3を入力手段9にて入力する必要がなくなる。この操作における利用者にデータおよびその認証データを公開することなく、それぞれの操作を遂行させることができる。また、従来の周辺装置8をPC1に接続する利用者にとっては従来同様に、外部記憶手段15に正規に記憶された認証データ3を入力しないと、PC1に登録されたデータ4に対する操作はできないという効果がある。

[0037] 従って、実施例1によれば、PC1の周辺装置8自体の使用許可の認証に使用される周辺装置認証データ16、PC1内で使用されるデータ4、及びPC1にて設定され、データ4に対してPC1との通信可否を認証する認証データ3を暗号化する暗号化手段10と、少なくとも暗号化された周辺装置認証データ16を記憶する外部記憶手段15と、少なくとも暗号化周辺装置認証データ17を記憶する内部記憶手段11と、周辺装置認証データ16、データ4、認証データ3を復号化する復号化手段12と、外部記憶手段15、内部記憶手段11から読み出された各々の復号化された周辺装置認証

データ16を照合してPC1の周辺装置8の使用可否を判別する照合手段とを備えたので、周辺装置の利用者に認証データ3およびデータ4の中身を公開する必要のないPC1の周辺装置8を提供することができる。

[0038] 実施例1によれば、PC1に関するデータの操作を制限する場合、あるいは，PC1への接続を制限する場合の、制限を解除する周辺装置認証データ16を最初に一度設定しておけば、その後の操作者に認証データ3そのものを公開しなくてもよくなり、セキュリティが向上する効果がある。

また、PC1に関するデータを暗号化して保存することで、情報資産としてのプログラムデータを、第三者の不正利用から守ることができる。

実施例 2

[0039] PC1と周辺装置8がネットワーク環境を経由して接続される場合について説明する。

構成としては、実施例1と同じであるが、周辺装置8とPC1との情報のやりとりに関しては、ネットワーク7に限定されているだけである。尚、図において表示していない部分については実施例1と同じであり、実施例2と実施例1における同一符号は、同一又は相当部分を示す。

PC1は、他の周辺装置8からネットワーク7を介して接続されてしまう可能性があるということを回避するため、ネットワーク7の接続自体の制限を実施するためのネットワーク認証データ18を設定することができる。図13は、本発明の実施例2におけるネットワーク7を介したPC1へのアクセス制御のための認証情報の設定時の説明図である。また、図14は、図13の説明図のフローチャートを示す。

[0040] 図13、図14において、ネットワーク認証データ18を設定するには、まず周辺装置8自体が、内部記憶手段11と外部記憶手段15とに記憶された暗号化周辺装置認証データ17同士を復号し、照合手段13による比較によって許可された状態であるかを判別した上で(S172)、入力手段9からネットワーク認証データ18が入力され(S173)、ネットワーク認証データ18は、PC1内の認証手段5にネットワーク7を介して転送され、登録される(S174)と共に、暗号化手段10がネットワーク認証データ18を暗号化して、内部記憶手段11または外部記憶手段15に保存される(S175)。S175までの

工程がすべて成功したことを確認し(S176)、成功していればネットワーク認証データ18の登録が終了する(S177)。S172での装置利用可能状態ではない場合はネットワーク認証データ18は、登録失敗となり(S179)、S174とS175での登録がいずれかが失敗していた場合はネットワーク認証データ18は、削除された上で(S178)、登録失敗となる。

[0041] また、PC1と周辺装置8がネットワーク環境を経由して接続される時、PC1への接続の制限を解除するためのネットワーク認証データ18を外部記憶手段15から取得して、PC1へ送信することができる。図15は、本発明の実施例2における周辺装置8のネットワーク7を介したPC1へのアクセスの説明図である。また、図16は、図15の説明図のフローチャートである。

[0042] ネットワーク7経由での接続の制限がかけられたPC1にアクセスする周辺装置8の利用者は、内部記憶手段11と外部記憶手段15とに記憶された暗号化された認証データ4同士を復号し、照合手段13による比較によって許可された状態であるかを判別した上で(S182)、ネットワーク7経由でPC1にアクセスする場合、内部記憶手段11又は外部記憶手段15内に記憶された暗号化されたネットワーク認証データ18を復号化手段12によって復号化し(S183)し、ネットワーク7経由でPC1に送信する(S184)。PC1の認証手段5は送信されたネットワーク認証データと事前に登録されているネットワーク認証データとを照合し(S185)、一致すればPC1への接続を許可する(S186)。S182において周辺装置8の利用が許可されていなかったり、S185のネットワーク認証データが一致しなかった場合は、PC1への接続を許可されない(S187)。

[0043] 従って、実施例2によれば、実施例1によって得られる効果だけでなく、PC1と周辺装置8との通信がネットワークによるものである場合に、PC1と周辺装置8との通信を可能とするためのネットワーク認証データ18を暗号化する暗号化手段10と、ネットワーク認証データ18が記憶される外部記憶手段15と、外部記憶手段15に記憶されたネットワーク認証データ18を復号化する復号化手段12とを備えたので、PC1と周辺装置8との通信がネットワークによるものであっても実施例1と同様の効果を得ることができる。

産業上の利用可能性

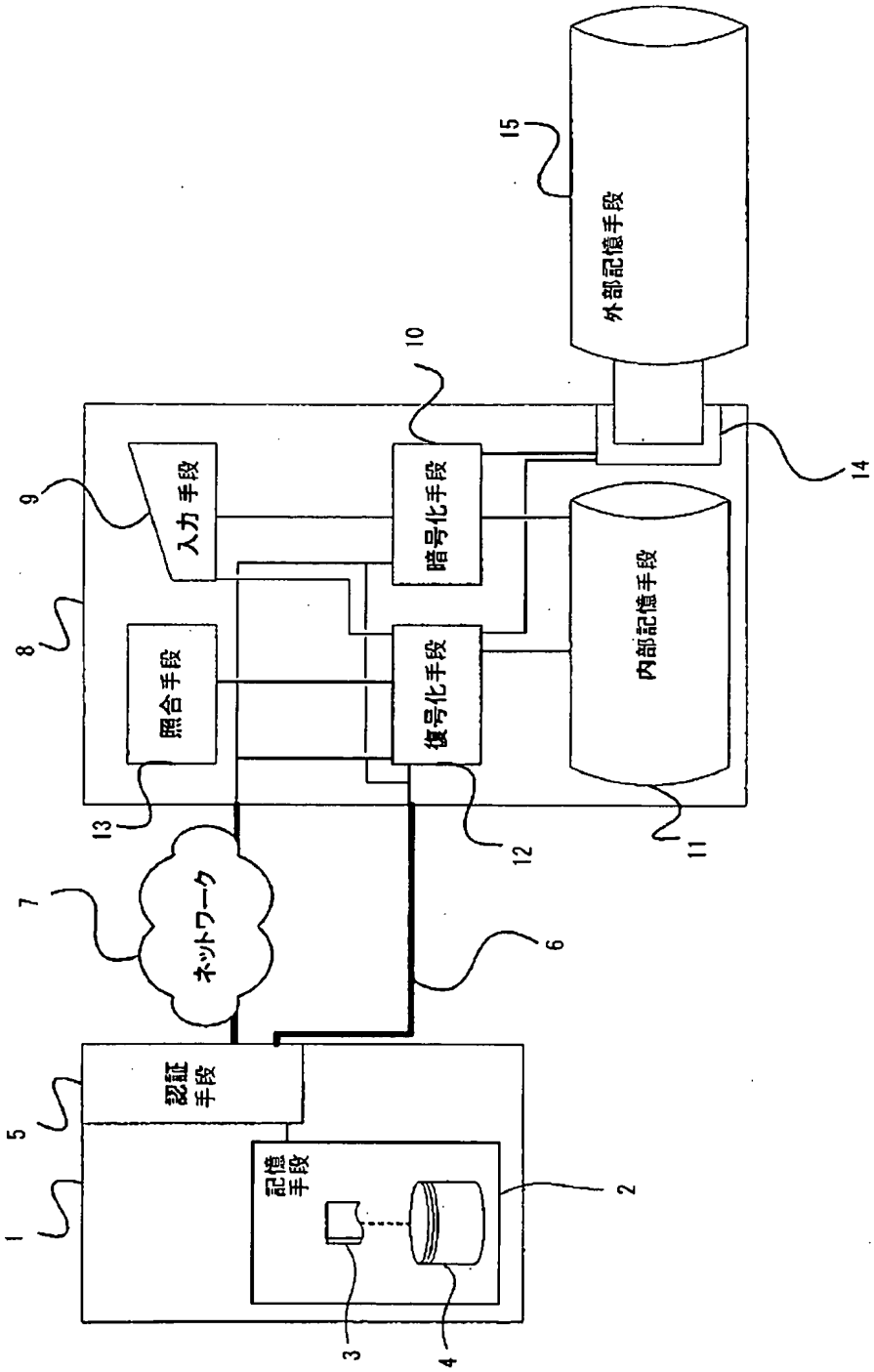
[0044] この発明に係るプログラマブルロジックコントローラの周辺装置は、プログラマブルロジックコントローラのプログラムなどの情報資産の秘匿に適している。

請求の範囲

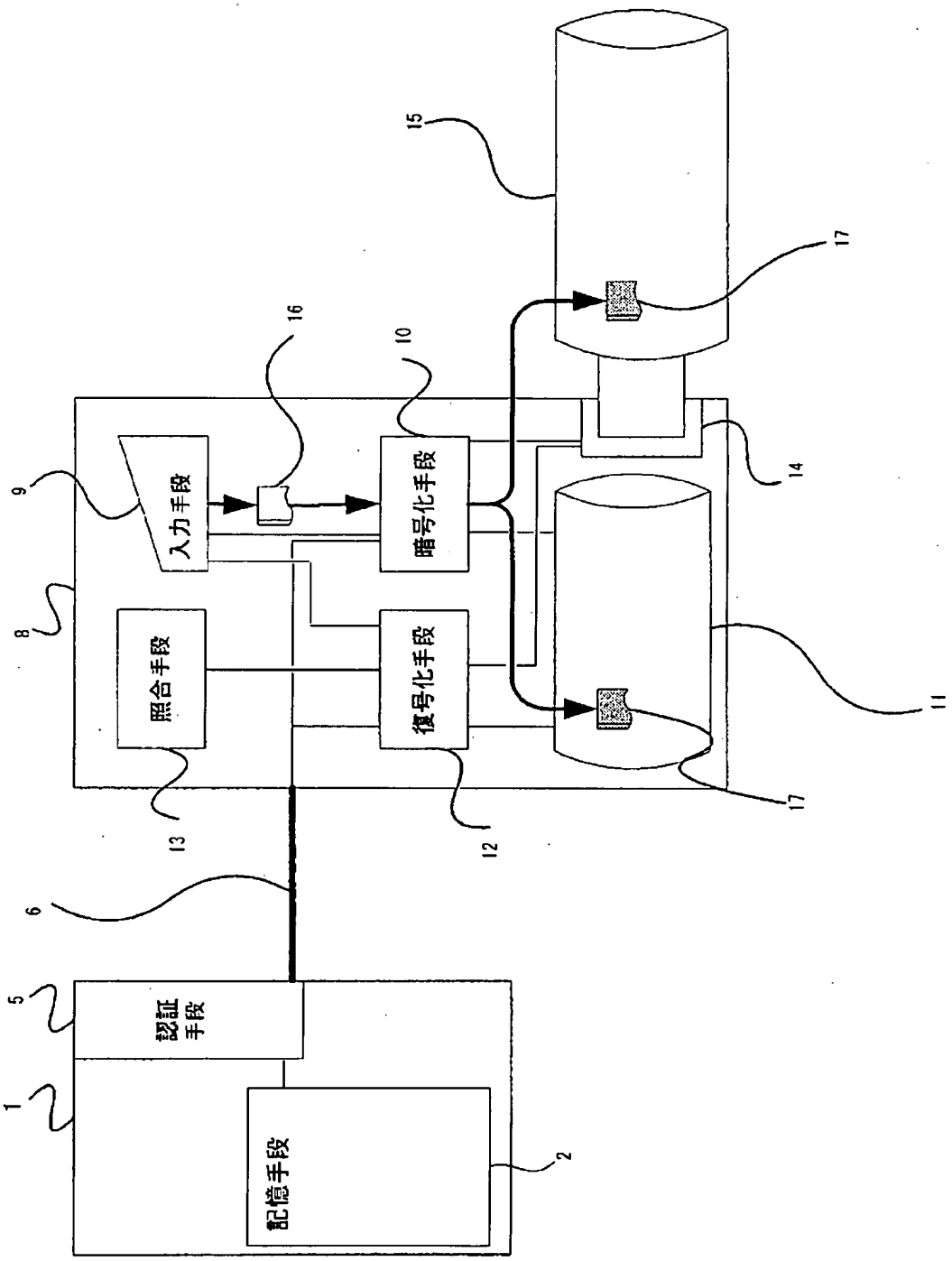
[1] プログラマブルロジックコントローラの周辺装置自体の使用許可の認証に使用される周辺装置認証データ、プログラマブルロジックコントローラ内で使用されるデータ、及び前記プログラマブルロジックコントローラにて設定され、プログラマブルロジックコントローラ内で使用される前記データに対してプログラマブルロジックコントローラとの通信可否を認証する認証データを暗号化する暗号化手段と、少なくとも暗号化された前記周辺装置認証データを記憶する外部記憶手段と、少なくとも暗号化された前記周辺装置認証データを記憶する内部記憶手段と、前記周辺装置認証データ、プログラマブルロジックコントローラ内で使用される前記データ、前記認証データを復号化する復号化手段と、前記外部記憶手段、前記内部記憶手段から読み出され、復号化された各々の前記周辺装置認証データを照合してプログラマブルロジックコントローラの周辺装置の使用可否を判別する照合手段とを備えたことプログラマブルロジックコントローラの周辺装置。

[2] プログラマブルロジックコントローラとプログラマブルロジックコントローラの周辺装置との通信がネットワークによるものである場合に、前記プログラマブルロジックコントローラと前記プログラマブルロジックコントローラの周辺装置との通信を可能とするためのネットワーク認証データを暗号化する前記暗号化手段と、前記ネットワーク認証データが記憶される前記外部記憶手段と、前記外部記憶手段に記憶された前記ネットワーク認証データを復号化する前記復号化手段とを備えたことを特徴とする請求項1に記載のプログラマブルロジックコントローラの周辺装置。

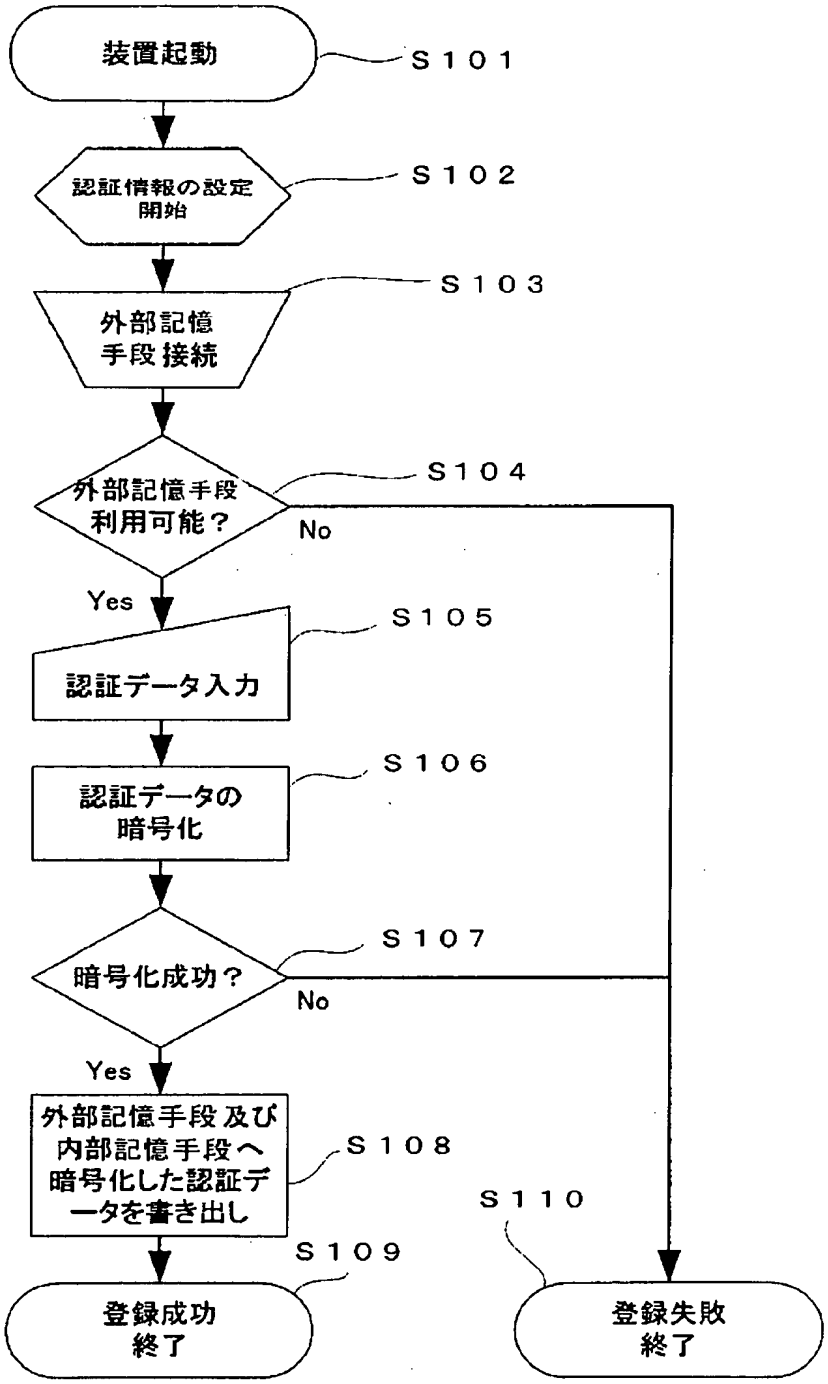
[図1]


外部記憶手段
15
10
入力手段
9
暗号化手段
14
8
照合手段
復号化手段
内部記憶手段
13
12
11
ネットワーク
7
6
認証手段
5
記憶手段
1
2
3
4

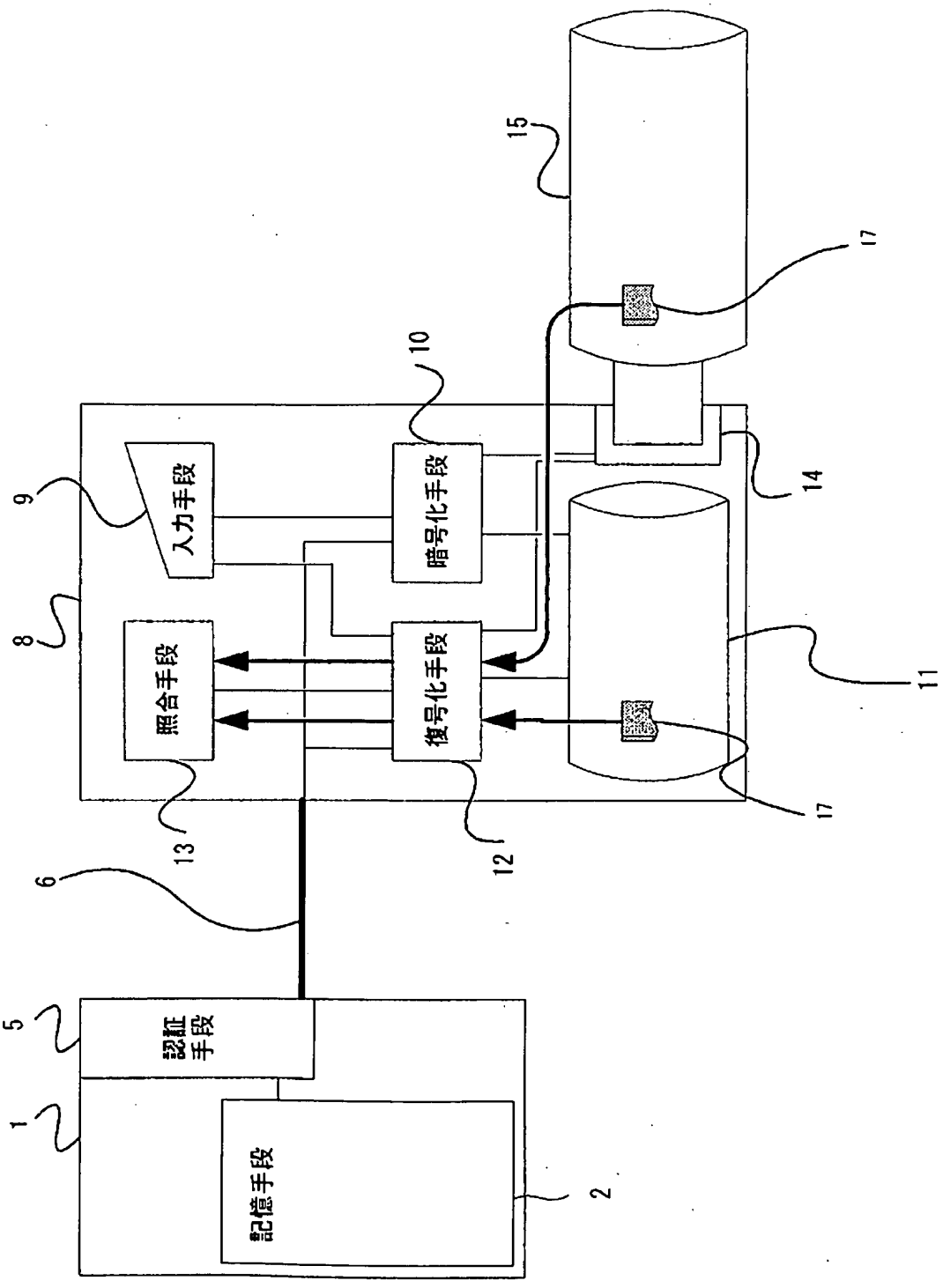
[図2]


15
17
16
10
9
入力手段
暗号化手段
14
8
照合手段
復号化手段
11
17
13
12
6
5
認証手段
1
記憶手段
2

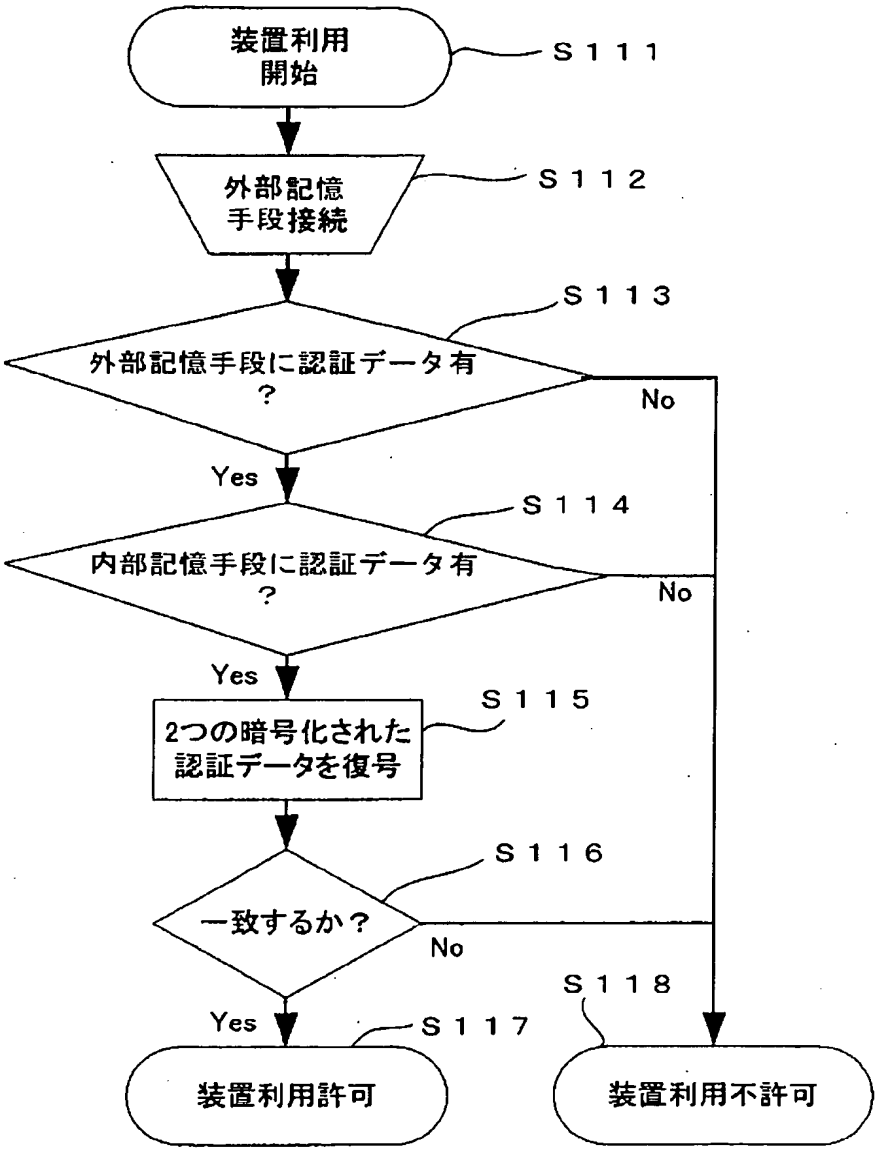
[図3]


装置起動
S101
認証情報の設定開始
S102
外部記憶手段接続
S103
外部記憶手段利用可能？
S104
No
Yes
認証データ入力
S105
認証データの暗号化
S106
暗号化成功？
S107
No
Yes
外部記憶手段及び内部記憶手段へ暗号化した認証データを書き出し
S108
S110
S109
登録成功終了
登録失敗終了

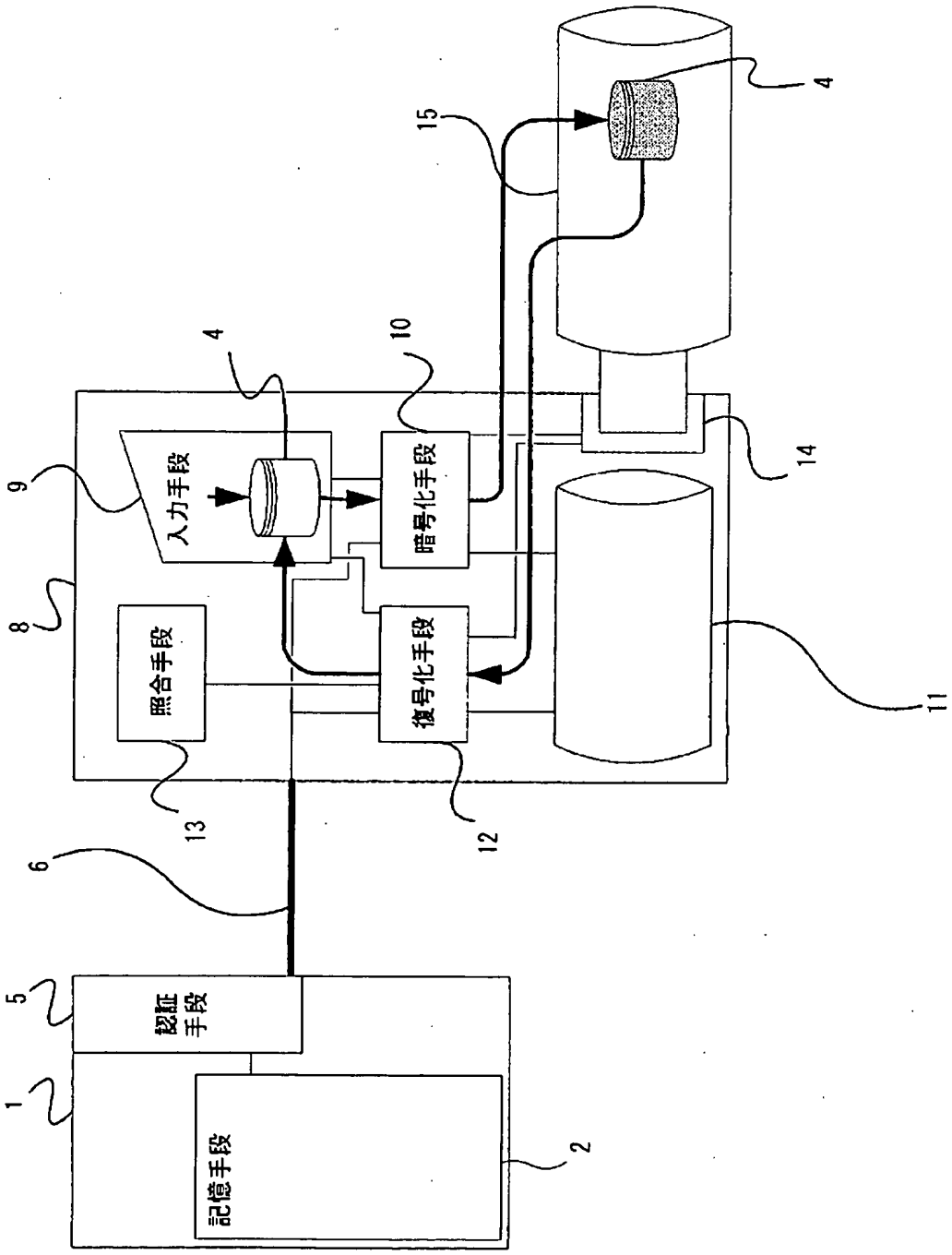
[図4]



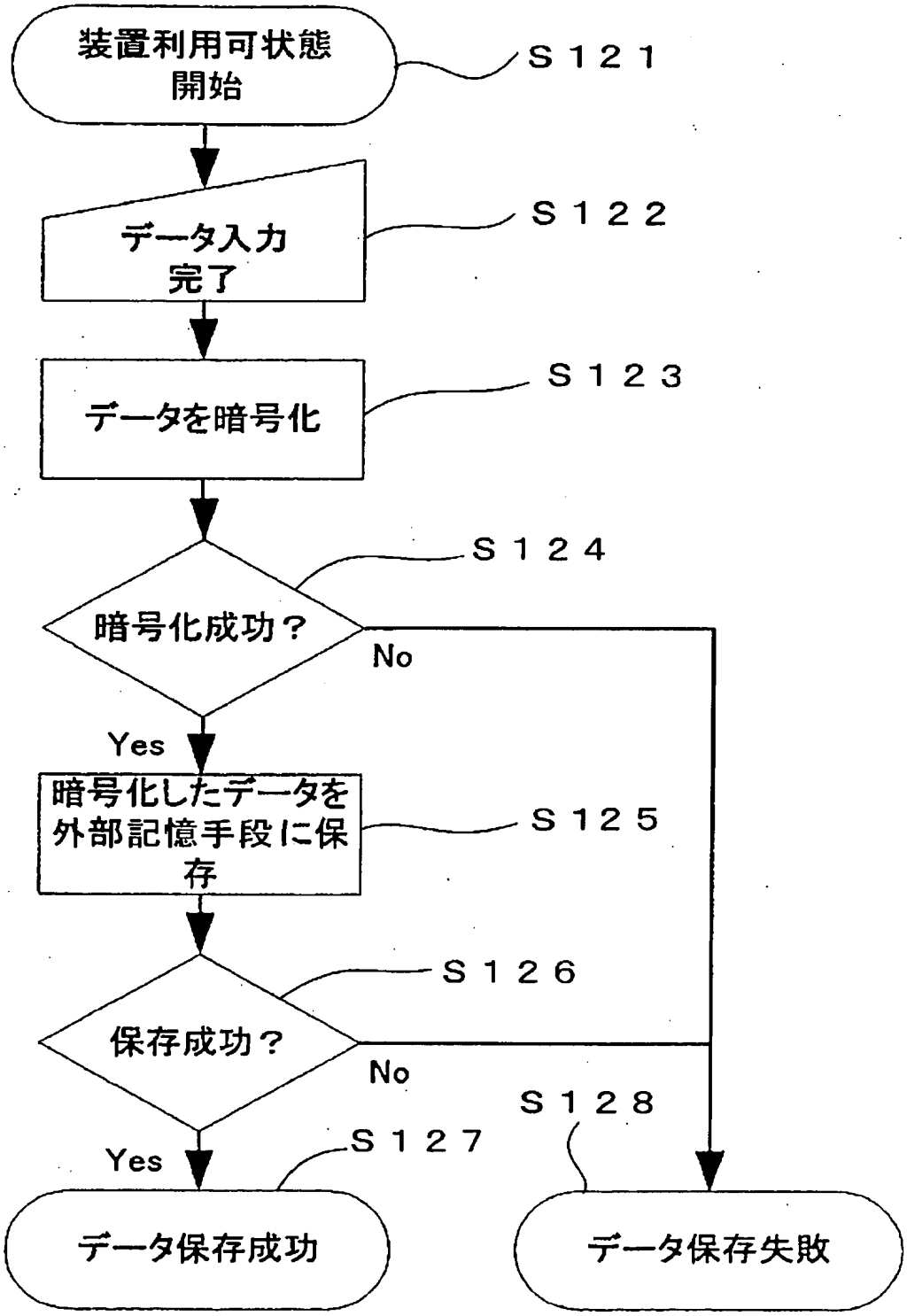
[図5]


装置利用開始
S111
外部記憶手段接続
S112
S113
外部記憶手段に認証データ有？
No
Yes
S114
内部記憶手段に認証データ有？
No
Yes
S115
2つの暗号化された認証データを復号
S116
一致するか？
No
S118
Yes
S117
装置利用許可
装置利用不許可

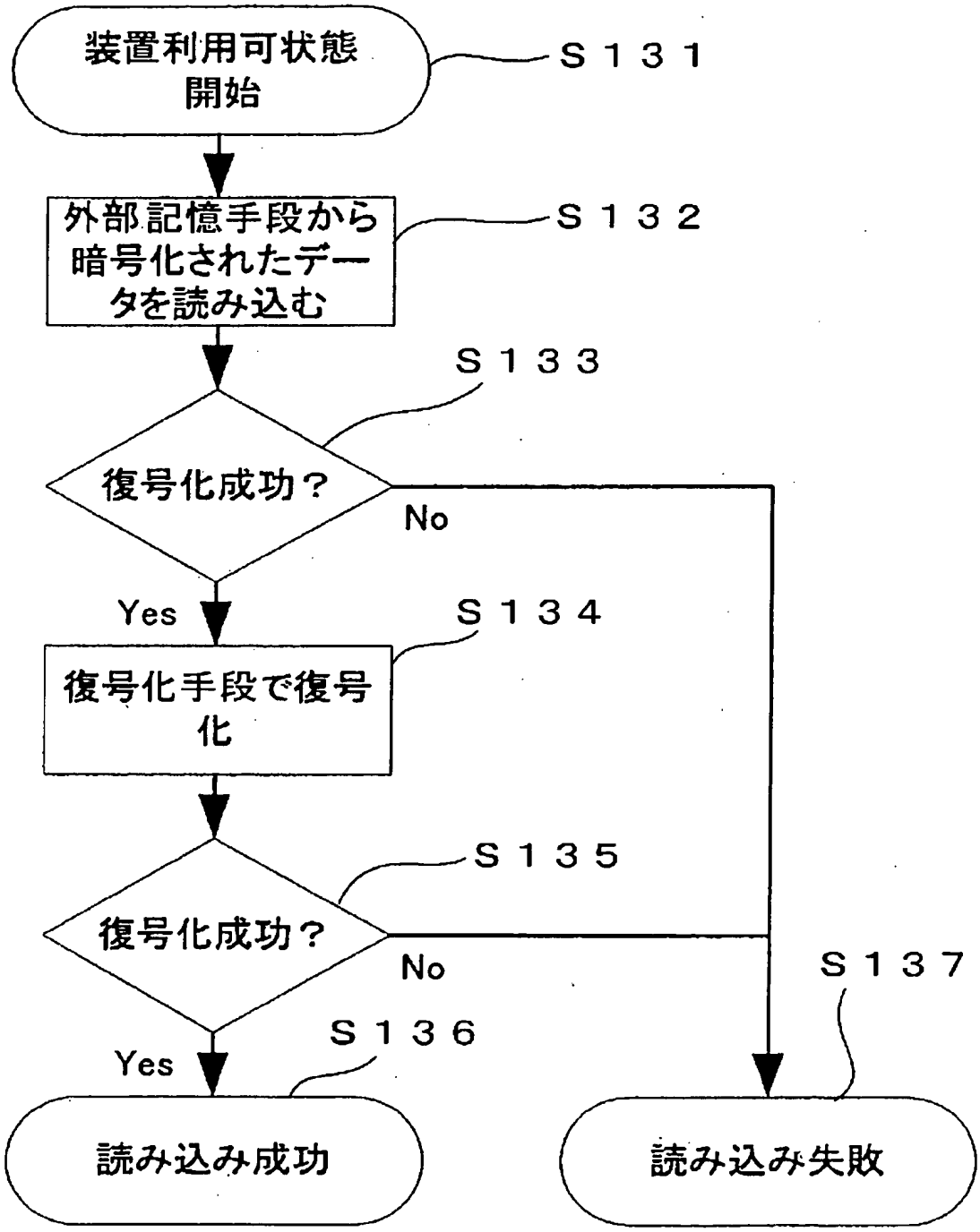
[図6]



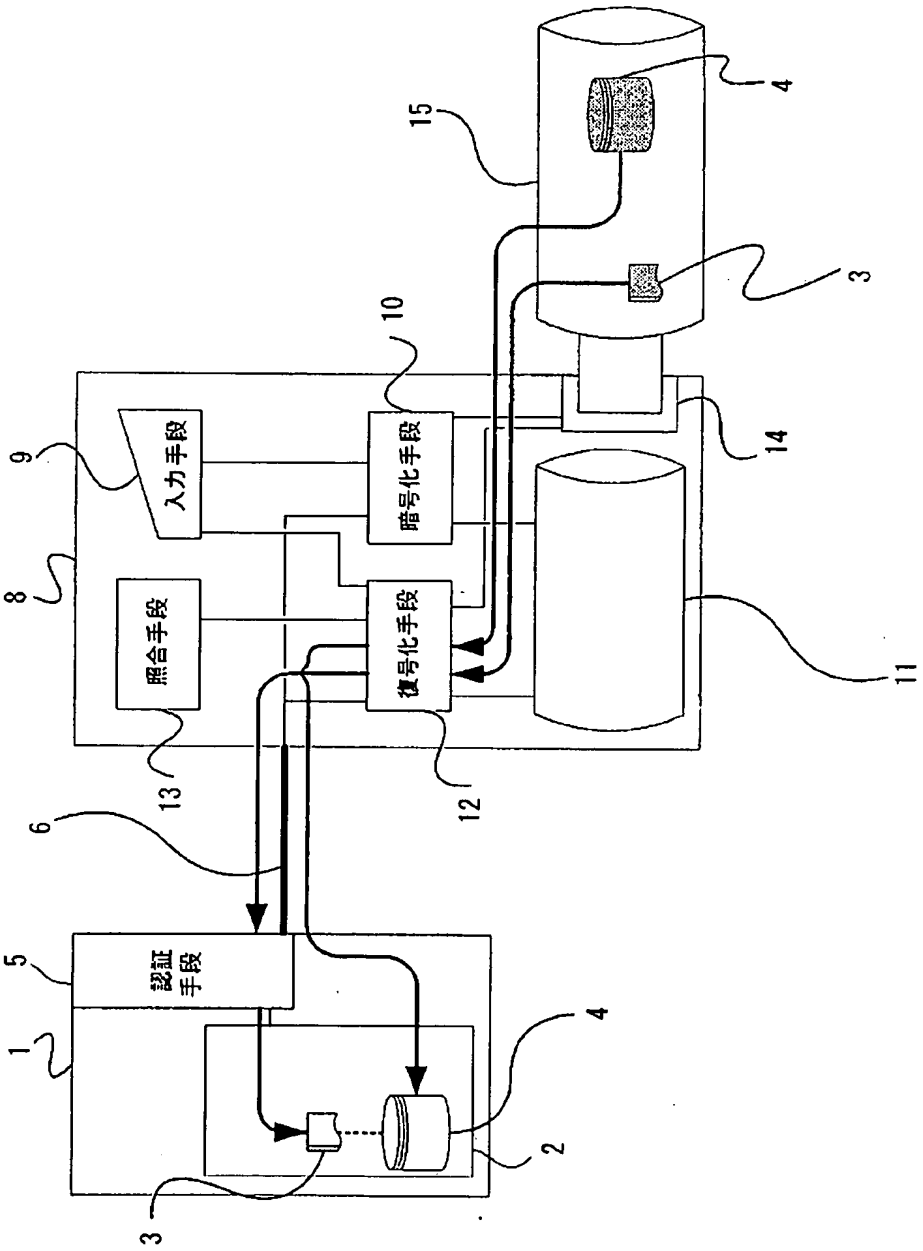
[図7]


装置利用可状態
開始
S121
データ入力
完了
S122
データを暗号化
S123
S124
暗号化成功？
No
Yes
暗号化したデータを
外部記憶手段に保
存
S125
S126
保存成功？
No
S128
Yes
S127
データ保存成功
データ保存失敗

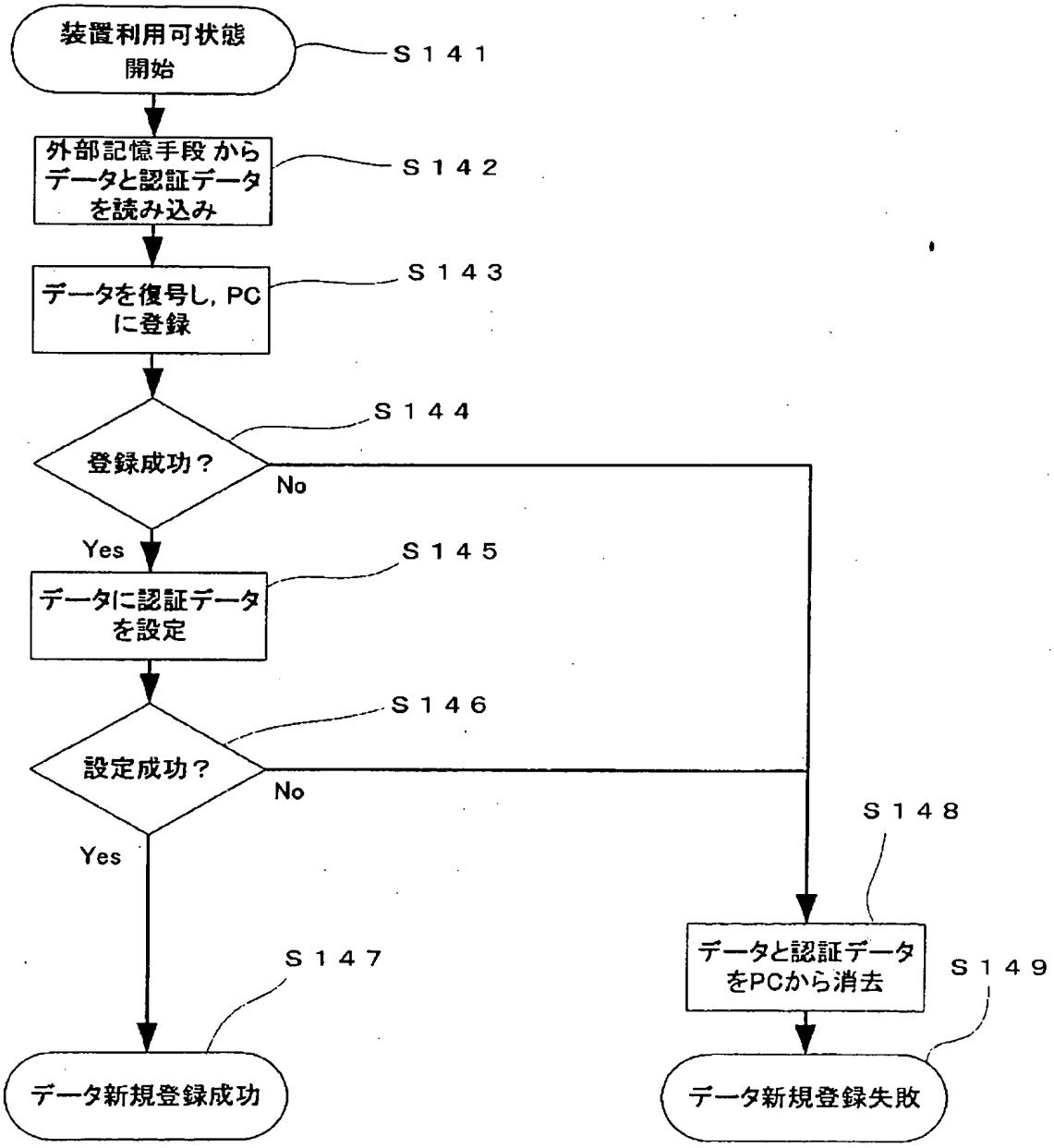
[図8]


装置利用可状態開始
S131
外部記憶手段から暗号化されたデータを読み込む
S132
S133
復号化成功？
No
Yes
S134
復号化手段で復号化
S135
復号化成功？
No
S137
Yes
S136
読み込み成功
読み込み失敗

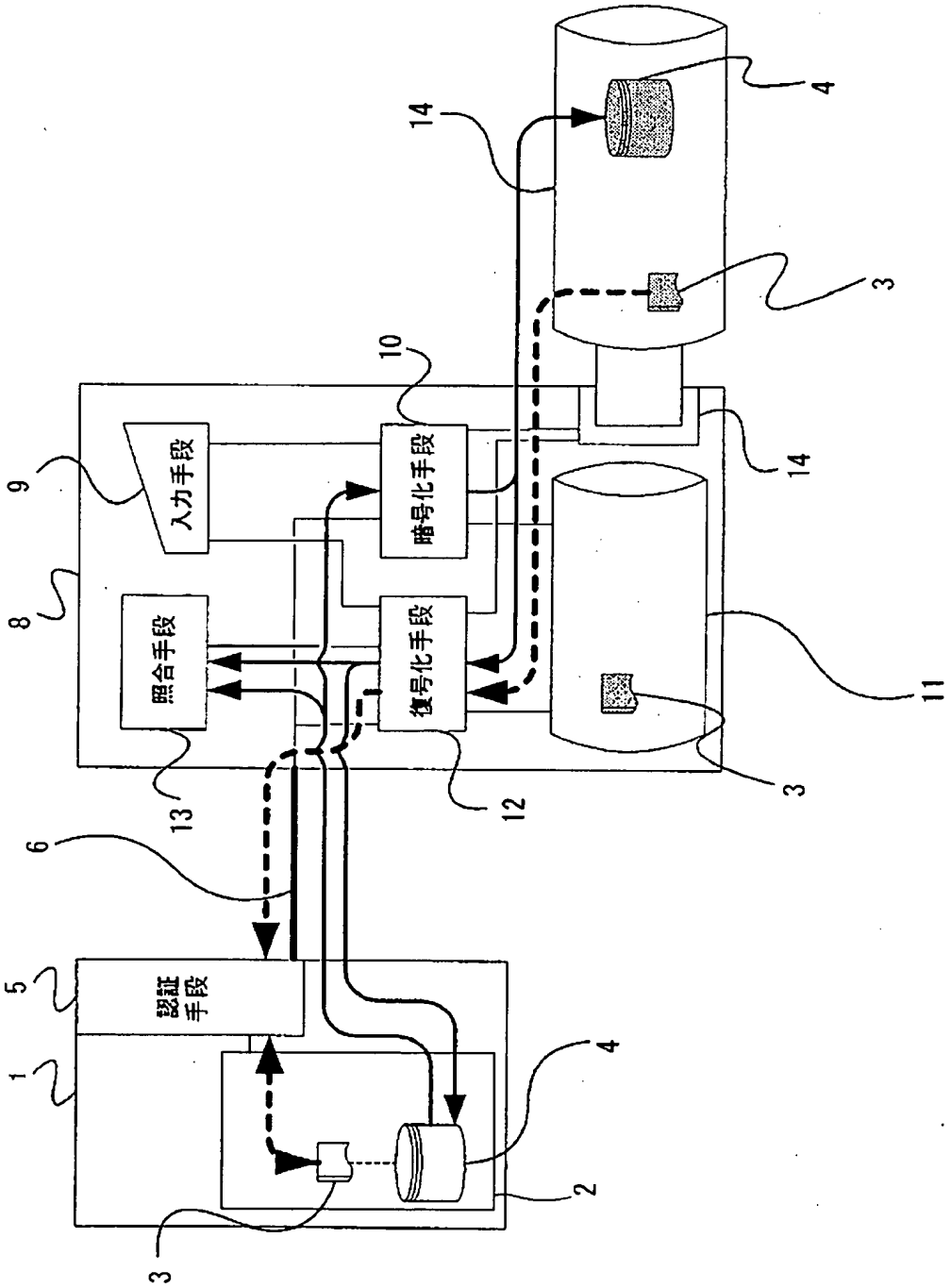
[図9]



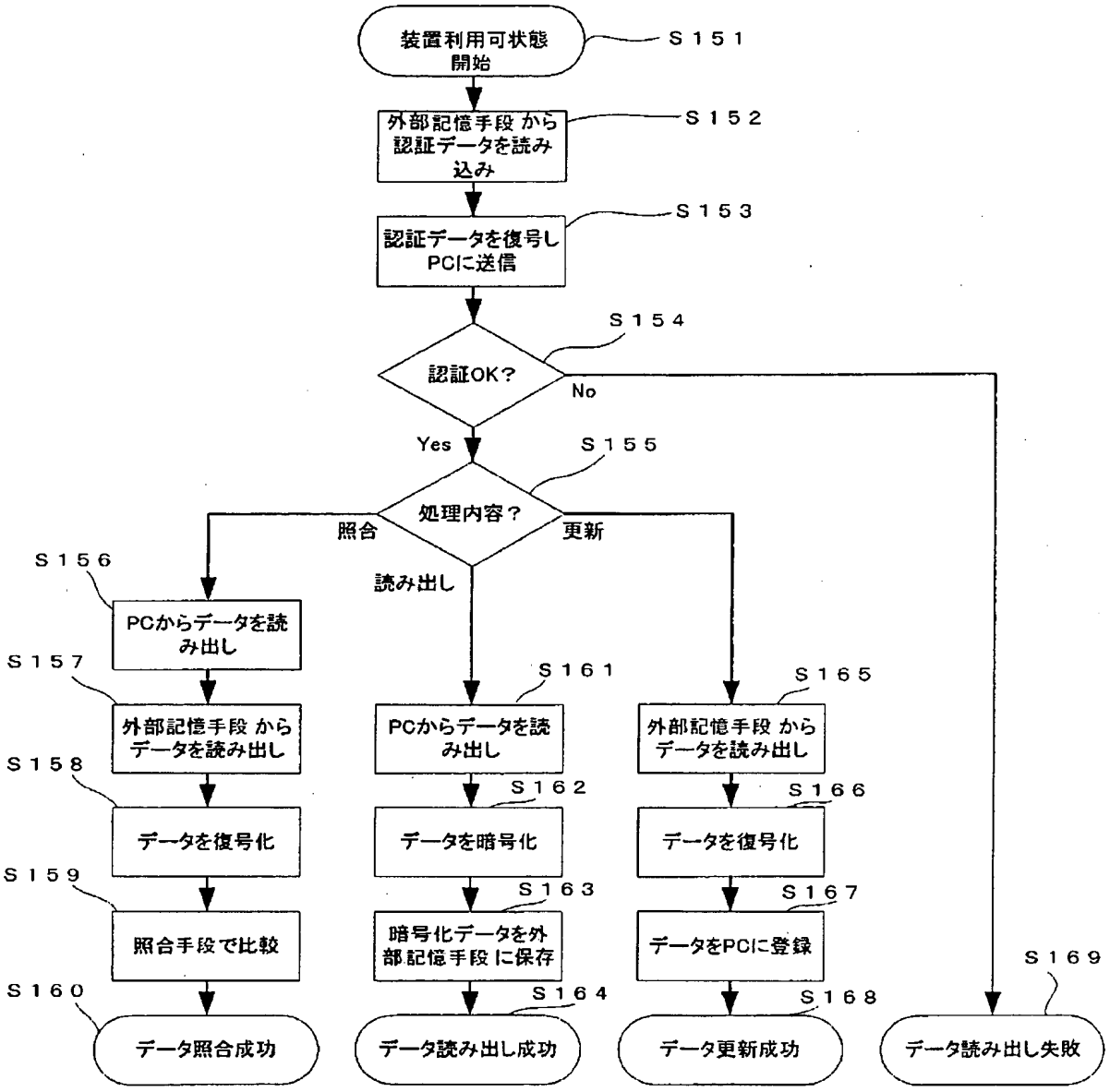
[図10]


装置利用可状態
開始
S141
外部記憶手段からデータと認証データを読み込み
S142
データを復号し, PCに登録
S143
登録成功？
S144
No
Yes
データに認証データを設定
S145
設定成功？
S146
No
Yes
S148
データと認証データをPCから消去
S149
S147
データ新規登録成功
データ新規登録失敗

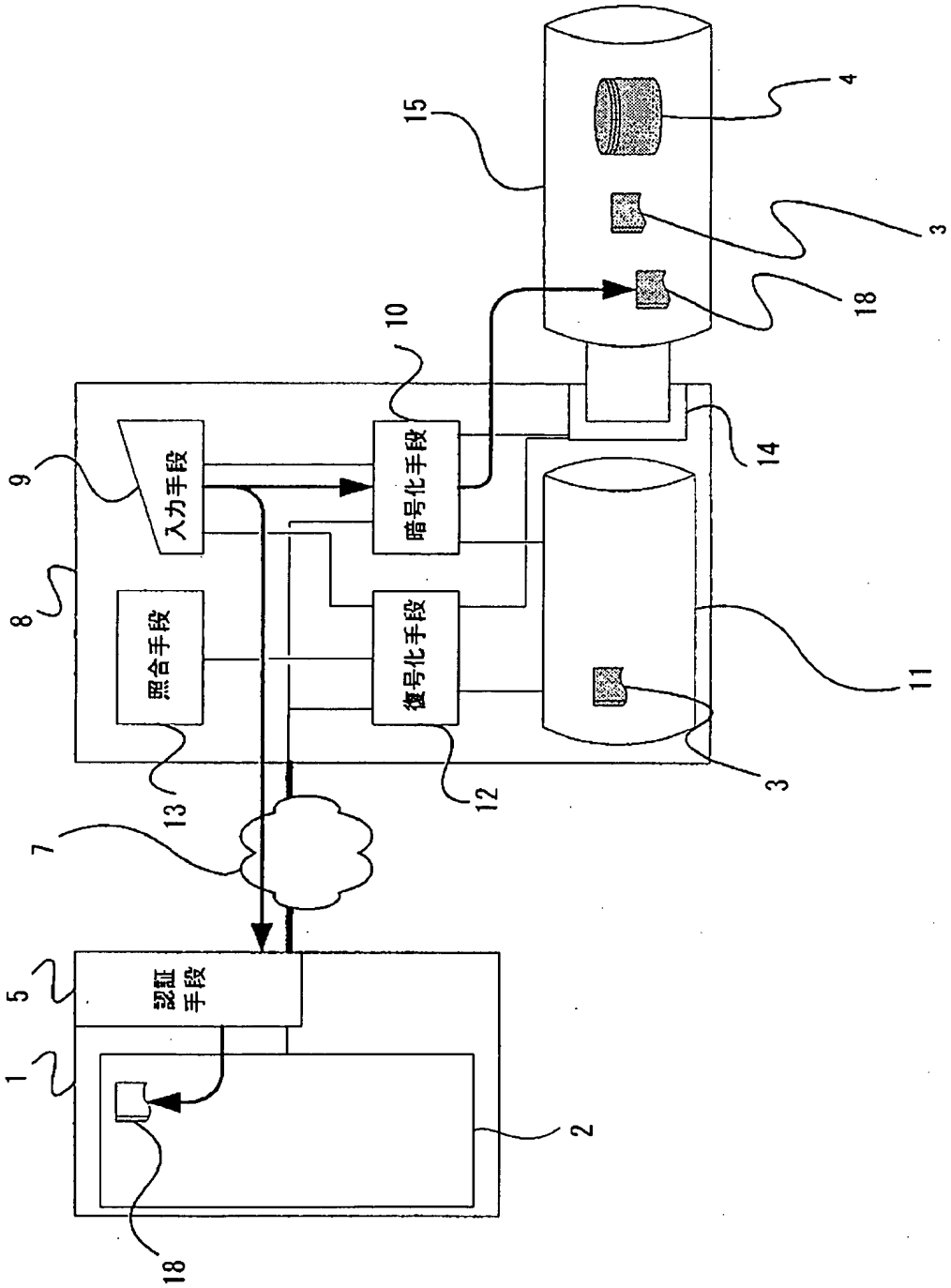
[図11]



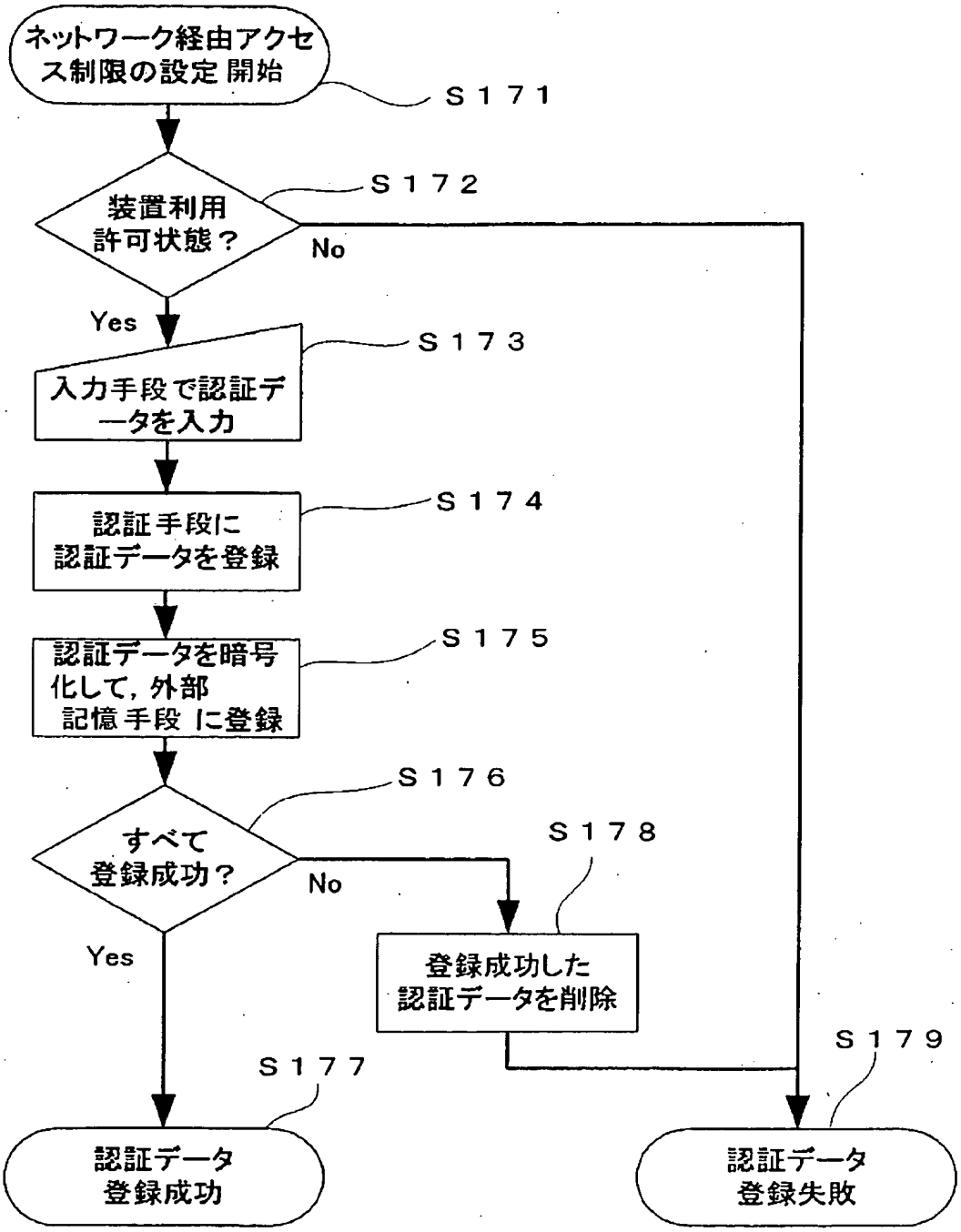
[図12]


装置利用可状態開始
S151
外部記憶手段から認証データを読み込み
S152
認証データを復号しPCに送信
S153
認証OK?
S154
No
Yes
処理内容?
S155
照合
読み出し
更新
S156
PCからデータを読み出し
S157
外部記憶手段からデータを読み出し
S158
データを復号化
S159
照合手段で比較
S160
データ照合成功
S161
PCからデータを読み出し
S162
データを暗号化
S163
暗号化データを外部記憶手段に保存
S164
データ読み出し成功
S165
外部記憶手段からデータを読み出し
S166
データを復号化
S167
データをPCに登録
S168
データ更新成功
S169
データ読み出し失敗

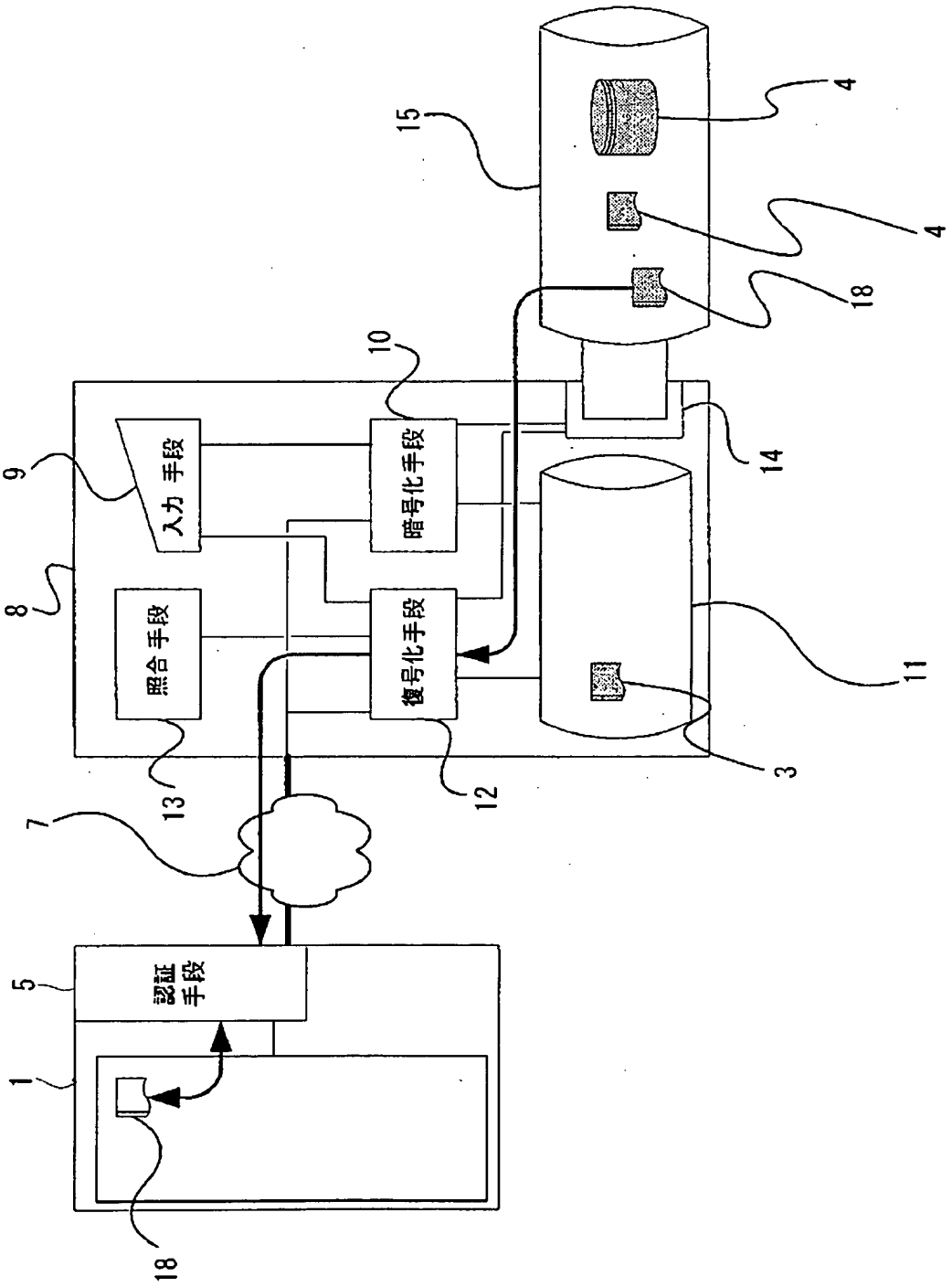
[図13]



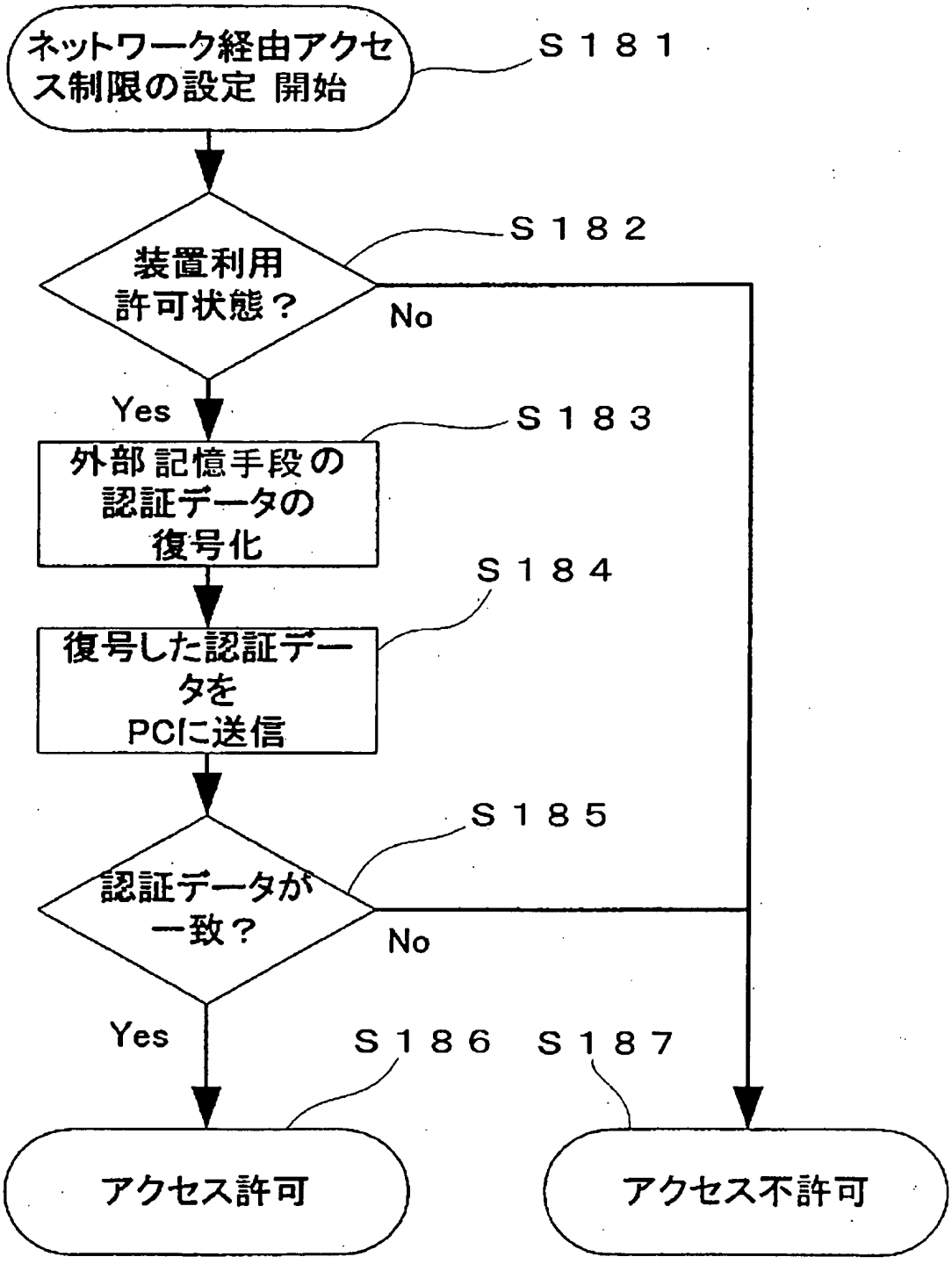
[図14]


ネットワーク経由アクセス制限の設定 開始
S171
装置利用許可状態？
S172
No
Yes
入力手段で認証データを入力
S173
認証手段に認証データを登録
S174
認証データを暗号化して，外部記憶手段 に登録
S175
すべて登録成功？
S176
No
Yes
S178
登録成功した認証データを削除
S179
S177
認証データ登録成功
認証データ登録失敗

[図15]



[図16]


ネットワーク経由アクセス制限の設定 開始
S１８１
装置利用許可状態？
S１８２
No
Yes
外部記憶手段の認証データの復号化
S１８３
復号した認証データをPCに送信
S１８４
認証データが一致？
S１８５
No
Yes
S１８６
S１８７
アクセス許可
アクセス不許可

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/000168

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F15/00, G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F15/00, G06F1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2005
Kokai Jitsuyo Shinan Koho 1971-2005 Toroku Jitsuyo Shinan Koho 1994-2005

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 10-124308 A (Mitsubishi Electric Corp.), 15 May, 1998 (15.05.98), Full text; all drawings (Family: none)	1,2
A	JP 2004-355223 A (NEC Corp.), 16 December, 2004 (16.12.04), Par. Nos. [0041] to [0054]; Figs. 2, 3 (Family: none)	1,2
A	JP 2004-15077 A (Mitsubishi Electric Corp.), 15 January, 2004 (15.01.04), Par. Nos. [0010] to [0019]; Figs. 1, 2 (Family: none)	1,2

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 March, 2005 (28.03.05)	19 April, 2005 (19.04.05)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.